REMARKS

This Application has been carefully reviewed in light of the Office Action mailed December 15, 2011. All pending Claims 1-20 were rejected in the Office Action. Independent Claims 1, 13, and 20 are herein amended, Claim 7 is cancelled without prejudice or disclaimer, and new independent Claim 21 is added. Applicants respectfully request reconsideration and allowance of all Claims 1-20.

Rejections under 35 U.S.C. § 112, second paragraph (indefiniteness)

Claim 13 was rejected under 35 U.S.C. §112, second paragraph, as allegedly being indefinite, due to lack of antecedent basis for the term "the die." Applicants herein amend Claim 13 to correct this clerical error.

Amended Independent Claims 1 and 20 are Allowable

Independent Claims 1 and 20 were rejected under 35 U.S.C. §103(a) as being obvious in view of *Candelore* (US 5,861,662) in view of *Yamauchi* (U.S. Patent Publication 2002/0040420).

In order to establish a prima facie case of obviousness, the references cited by the Examiner must disclose all claimed limitations. *In re Royka*, 490 F.2d 981, 180 U.S.P.Q. 580 (C.C.P.A. 1974). Even if each limitation is disclosed in a combination of references, however, a claim composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art. *KSR Int'l. Co. v. Teleflex Inc.*, 127 S.Ct. 1727, 1741 (2007). Rather, the Examiner must identify an apparent reason to combine the known elements in the fashion claimed. *Id.* "Rejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *Id.*, citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006). Finally, the reason must be free of the distortion caused by hindsight bias and may not rely on ex post reasoning. *KSR*, 127 S.Ct. at 1742.

Although Applicants do not necessarily agree with the rejection of Claims 1 and 20, Applicants have amended Claims 1 and 20 to further distinguish from *Candelore* and *Yamauchi*, as discussed below.

Amended Claim 1

Amended Claim 1 recites in part:

> a security sensor system including a protective layer on the integrated circuit including at least one elongated electrical line extending along the surface of the integrated circuit, the security sensor system operable to:
>
> **monitor an ohmic resistance of at least one electrical line** of the protective layer on the integrated circuit,
>
> compare the monitored ohmic resistance of the at least one electrical line with a **threshold resistance value**,
>
> **detect a breaking of the electrical line based on the comparison**, and
>
> when a breaking of the electrical line is detected, automatically initiate the deletion of data from at least one memory of the integrated circuit.

Candelore and *Yamauchi* fail to teach these limitations. With respect to Claim 1, the Examiner cites *Candelore*'s shield 230, which is a metal layer that provides current to various components within an IC 200. If power to the shield is interrupted, than a secured processing component may self-destruct, such that cryptographic data stored in the processor is erased. The Examiner further refers to *Candelore*'s teaching that "The voltage V_{batt} may be used to provide a current which, when terminated, triggers an automatic erasure (e.g., self-destruct) feature of the processor 150." (Office Action, page 5). Further, with respect to dependent Claim 7 (which recited comparing a monitored operating parameter with a limit value and deleting the content of the first memory when the operating parameter exceeds or drops below the limit value), the Examiner cited *Anderson* (US 2003/0084336), paragraphs 0014-0015, which teach monitoring a number of instructions executed by a processor, or monitoring over- and under-voltage and low temperature, and triggering an alarm based on such monitored parameters.

However, neither *Candelore* nor *Anderson* teaches or even hints at **monitoring an ohmic resistance of an electrical line of a protective layer** on a integrated circuit, much less **comparing a monitored ohmic resistance with a threshold resistance value**, and detecting a breaking of the electrical line of a protective layer based on the comparison. Thus, amended Claim 1 is allowable over *Candelore* and *Yamauchi*. Therefore, Applicants respectfully request allowance of Claim 1, as well as all claims that depend therefrom.

Amended Claim 20

Amended Claim 20 recites, in combination with the other recited security features of the integrated circuit:

> **an integrated voltage regulator that regulates an operating voltage or current of the integrated circuit to render the operating voltage or current noisy to an outside observer, thus preventing attacks based on examination of the current of the integrated circuit.**

Candelore and *Yamauchi* fail to teach anything similar to an integrated voltage regulator that regulates an operating voltage or current of an IC to render the operating voltage or current noisy to an outside observer, thus preventing attacks based on examination of the current of the integrated circuit. Thus, Applicants respectfully request allowance of Claim 20.

<u>All Dependent Claims are Allowable.</u>

Dependent Claims 2-4, 6, and 8-19 were rejected under 35 U.S.C. §103(a) as being obvious in view of *Candelore* in view of *Yamauchi.*

Dependent Claim 5 was rejected under 35 U.S.C. §103(a) as being unpatentable over *Candelore* in view of *Yamauchi*, and further in view of *Nakajima* (U.S. Patent Publication 2004/0106239).

Dependent Claim 7 was rejected under 35 U.S.C. §103(a) as being unpatentable over *Candelore* in view of *Yamauchi*, and further in view of *Anderson* (U.S. Patent Publication 2003/0084336). Dependent Claim 7 is now cancelled, and the aspect of the rejection concerning *Anderson* is discussed above with reference to amended Claim 1.

Applicants submit that all dependent claims are allowable at least because they depend from independent Claim 1, which is shown above to be allowable. In addition, *Nakajima* and *Anderson* also fail to teach the limitations of Claims 1 and 20 discussed above. Further, Applicants do not concede that any of the combinations of references proposed by the Examiner are legally proper.

Thus, for at least these reasons, Applicants respectfully request reconsideration and allowance of all dependent claims.

New Claim 21 is Allowable.

New Claim 21 recites:

> 21. An integrated circuit system including:
>
> an integrated circuit comprising:
>
> . . .
>
> a first memory storing a cryptographic key,
>
> an encryption unit designed to encrypt and decrypt data using the cryptographic key stored in the first memory,
>
> a security sensor system including a **protective layer covering the integrated circuit** and a monitoring system that monitors the state of the protective layer covering the integrated circuit such that when a particular state of the protective layer is detected, data is automatically deleted from at least one memory of the integrated circuit, and
>
> at least one **terminal contact extending through the protective layer covering the integrated circuit**, and
>
> **an external second memory outside the protective layer covering the integrated circuit and connected to the integrated circuit via the at least one terminal contact extending through the protective layer, and connected to the encryption unit of the integrated circuit via a data bus extending through the at least one terminal contact, the external second memory storing data encrypted with the cryptographic key stored in the first memory**,
>
> **wherein the encryption unit is designed to read data or code out of the external second memory, decrypt the data or code using the cryptographic key stored in the first memory, and write the decrypted data or code into the first memory or other memory of the integrated circuit**.

Candelore and *Yamauchi* fail to teach (a) an IC covered by a protective coating, but with terminal contact(s) extending through the protective layer, (b) an external memory outside the covered IC and connected to the IC via the terminal contact(s), and storing data encrypted with a cryptographic key stored on the covered IC, and (c) an encryption unit on the covered IC that reads encrypted data from the external memory, decrypts the data using the locally-stored cryptographic key, and stores the decrypted data locally. Neither *Candelore* or *Yamauchi* (or any other cited reference) teaches anything similar.

Therefore, Applicants respectfully request allowance of Claim 20, as well as all claims that depend from Claim 20.

CONCLUSION

Applicants have made an earnest effort to place this case in condition for allowance in light of the remarks set forth above. Applicants respectfully request reconsideration of the pending claims.

Applicants believe there are no fees due at this time. However, the Commissioner is hereby authorized to charge any fees necessary or credit any overpayment to Deposit Account No. 50-4871 of King & Spalding L.L.P.

If there are any matters concerning this Application that may be cleared up in a telephone conversation, please contact Applicants' attorney at 512-457-2030.

Respectfully submitted,
KING & SPALDING LLP
Attorney for Applicants

Eric M Grabski
Registration No. 51,749

Date: 1/20/12

SEND CORRESPONDENCE TO:
KING & SPALDING L.L.P.
CUSTOMER ACCOUNT NO. **86528**
512-457-2030
512-457-2100 (fax)